FIG. 1

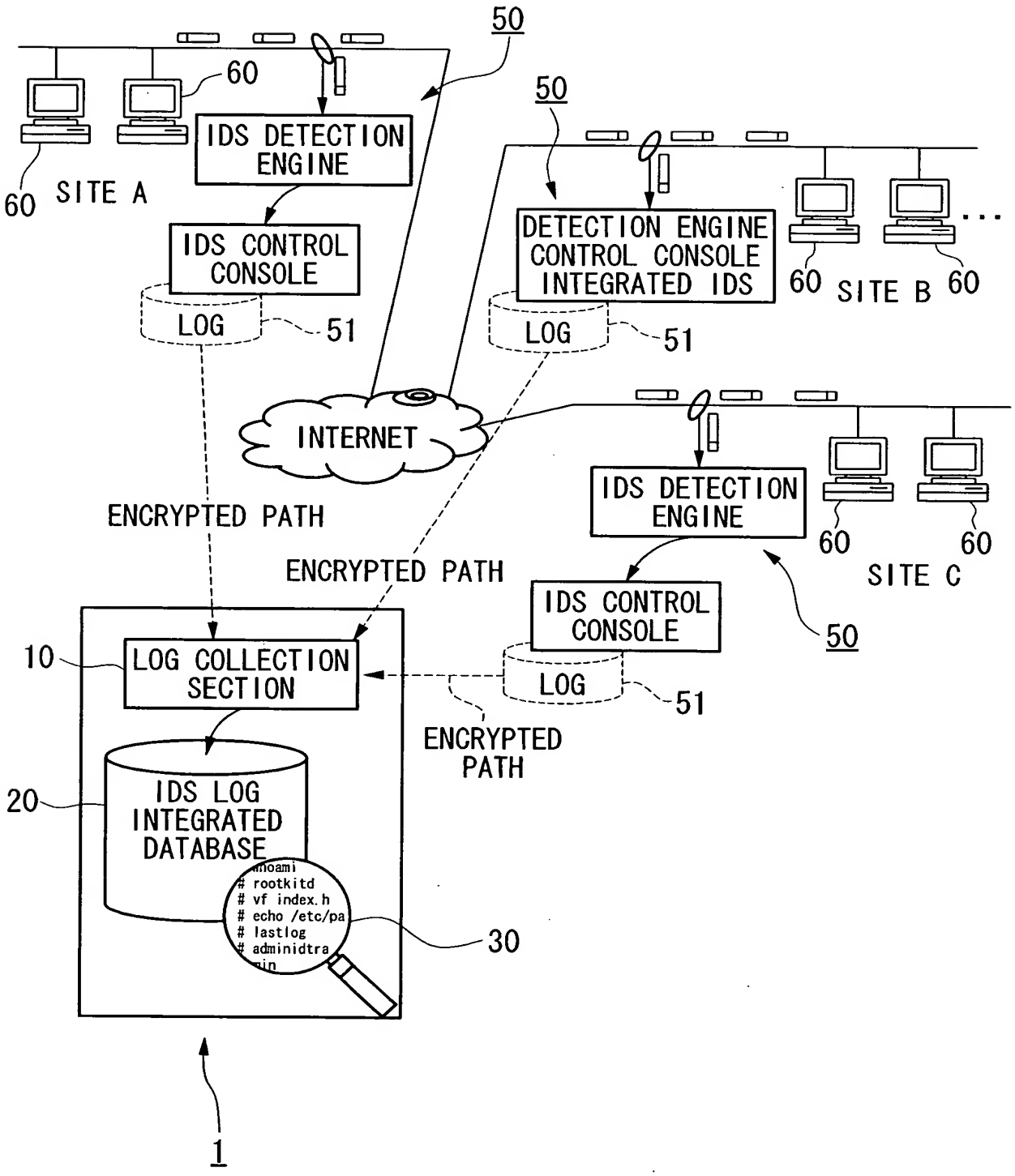
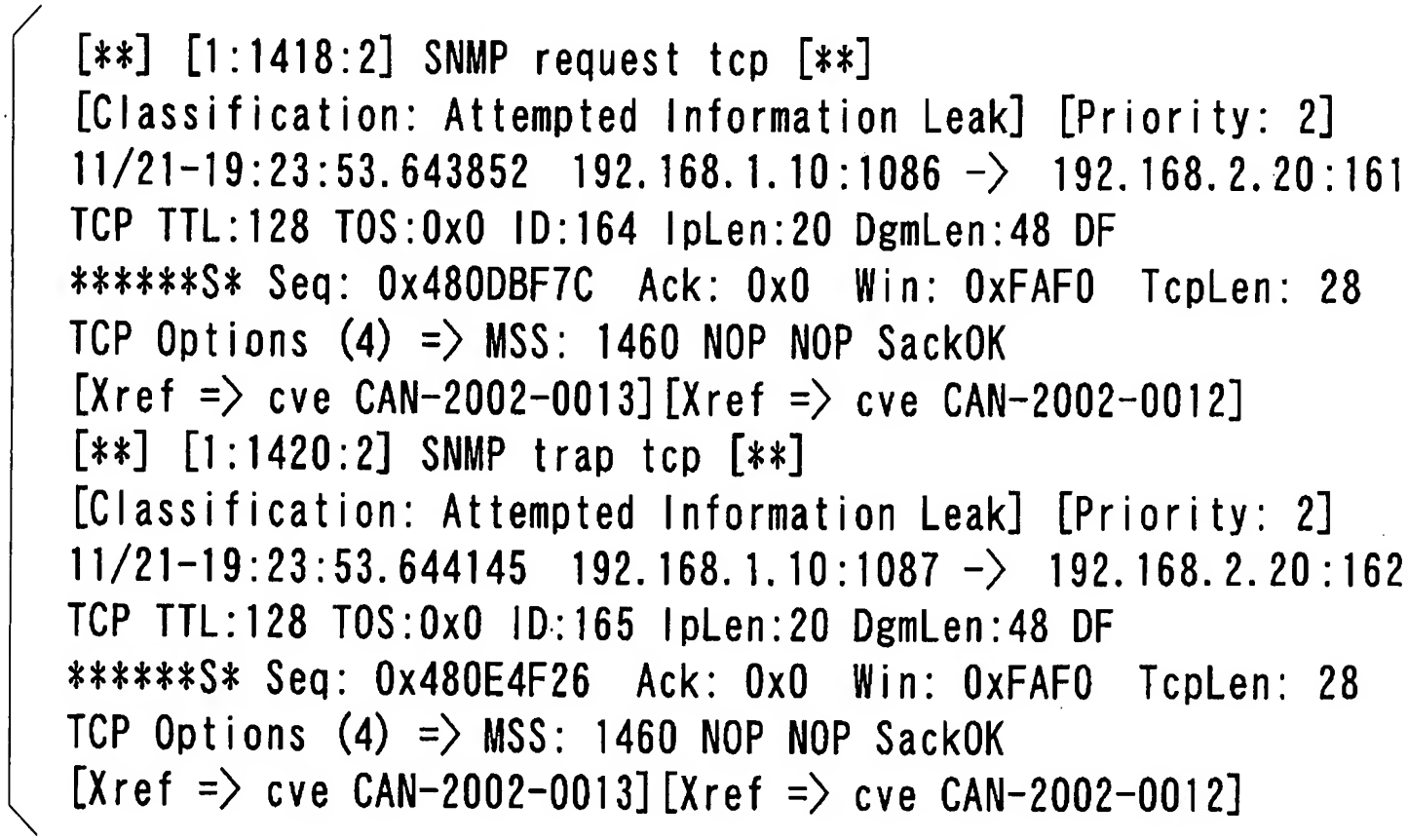

50
60
IDS DETECTION ENGINE
60
SITE A
IDS CONTROL CONSOLE
LOG
51
50
DETECTION ENGINE CONTROL CONSOLE INTEGRATED IDS
60
SITE B
60
LOG
51
INTERNET
ENCRYPTED PATH
IDS DETECTION ENGINE
60
60
SITE C
ENCRYPTED PATH
IDS CONTROL CONSOLE
50
10
LOG COLLECTION SECTION
LOG
51
ENCRYPTED PATH
20
IDS LOG INTEGRATED DATABASE
whoami
rootkitd
vf index.h
echo /etc/pa
lastlog
adminidtra
30
1

FIG. 2



```
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/21-19:23:53.643852  192.168.1.10:1086 -> 192.168.2.20:161
TCP TTL:128 TOS:0x0 ID:164 IpLen:20 DgmLen:48 DF
******S* Seq: 0x480DBF7C  Ack: 0x0  Win: 0xFAF0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
[Xref => cve CAN-2002-0013][Xref => cve CAN-2002-0012]
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/21-19:23:53.644145  192.168.1.10:1087 -> 192.168.2.20:162
TCP TTL:128 TOS:0x0 ID:165 IpLen:20 DgmLen:48 DF
******S* Seq: 0x480E4F26  Ack: 0x0  Win: 0xFAF0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
[Xref => cve CAN-2002-0013][Xref => cve CAN-2002-0012]
```

FIG. 3

Event ID	IDS ID	Signature ID	Time	Source IP	Source Port	Destination IP	Destination Port	IP Protocol
1	1	26	2002/5/3 5:42	192.168.10.33	5963	127.0.0.137	53	UDP
2	1	12	2002/5/3 5:45	192.168.10.33	1766	127.0.0.138	5631	TCP
3	1	16	2002/5/3 5:45	127.0.0.140	1767	192.168.45.34	111	TCP
4	1	3	2002/5/3 5:45	192.168.10.36	1935	127.0.0.139	12345	TCP
5	1	11	2002/5/3 5:45	192.168.10.37	1972	127.0.0.140	53	TCP
6	1	102	2002/5/3 5:45	192.168.10.38	1977	127.0.0.141	698	TCP
7	1	301	2002/5/3 5:45	192.168.10.39	3333	127.0.0.142	137	TCP
8	2	302	2002/5/3 5:45	192.168.10.38	2222	127.0.0.141	138	TCP
9	2	26	2002/5/3 5:48	192.168.10.38	1111	127.0.0.141	53	UDP
10	2	526	2002/5/3 5:48	192.168.10.38	60171	127.0.0.141	80	TCP
11	1	301	2002/5/3 5:48	127.0.0.141	2002	192.168.10.38	-1	TCP
12	2	526	2002/5/3 5:48	192.168.10.38	60171	127.0.0.141	80	TCP
13	2	17	2002/5/3 5:48	192.168.10.38	3317	127.0.0.141	1080	TCP
14	2	18	2002/5/3 5:48	192.168.10.38	3391	127.0.0.141	1723	TCP
15	1	102	2002/5/3 5:48	127.0.0.142	3415	192.168.0.12	385	TCP
16	1	301	2002/5/3 5:48	192.168.10.35	5963	127.0.0.139	137	TCP

FIG. 4

IDS ID	Signature ID	Signature Name	Severity
1	1	TCP port probe	1
1	2	UDP port probe	1
1	3	PCAnywhere port probe	1
1	4	RPC TCP port probe	1
1	5	NetBus port probe	2
1	6	DNS TCP port probe	1
1	7	DNS UDP port probe	1
1	8	TCP port scan	2
1	9	UDP port scan	2
1	10	TCP SYN flood	3
1	11	Telnet port probe	2
1	12	NMAP ping	3

FIG. 5

Event ID	Parameter	
	Name	Value
2	port	5631
2	reason	RSTsent
3	port	111
3	reason	RSTsent
4	port	12345
4	name	NetBus
4	reason	RSTsent
5	port	53
5	reason	RSTsent
6	port	1-93, 131-403, 441-723, 765-1019, 1067-1110, 1248, 1356
6	reason	RSTsent
7	port	2-3, 5, 8-9, 11-15, 17, 19-21, 23-28, 30-32, 35-36, 40-43,
8	PercentFromIntruder	99-100
8	SYNs	214
8	DATAs	0
10	count	2

FIG. 6

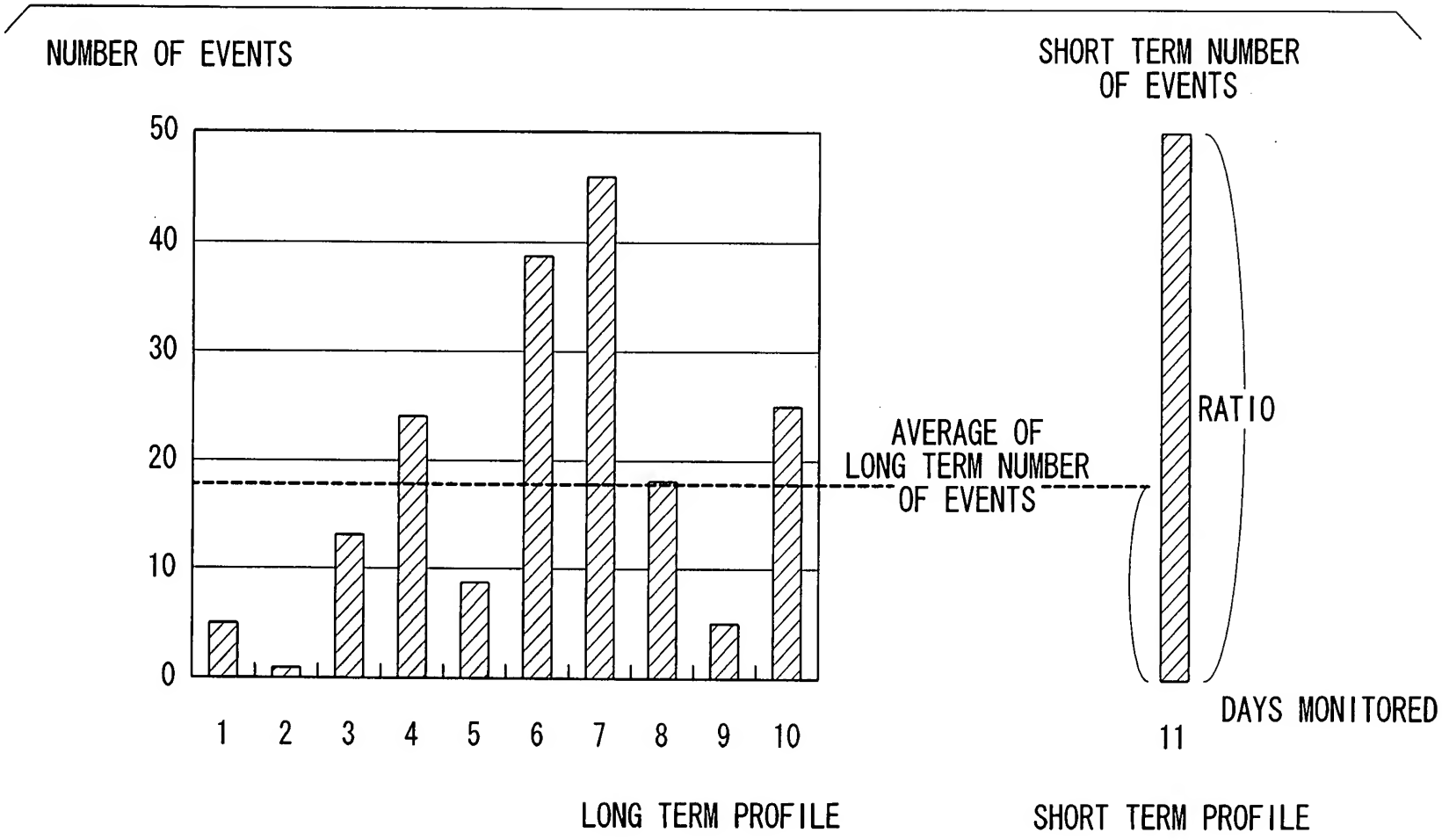

NUMBER OF EVENTS
SHORT TERM NUMBER OF EVENTS
50
40
30
20
10
0
AVERAGE OF LONG TERM NUMBER OF EVENTS
RATIO
1
2
3
4
5
6
7
8
9
10
11
DAYS MONITORED
LONG TERM PROFILE
SHORT TERM PROFILE

FIG. 7

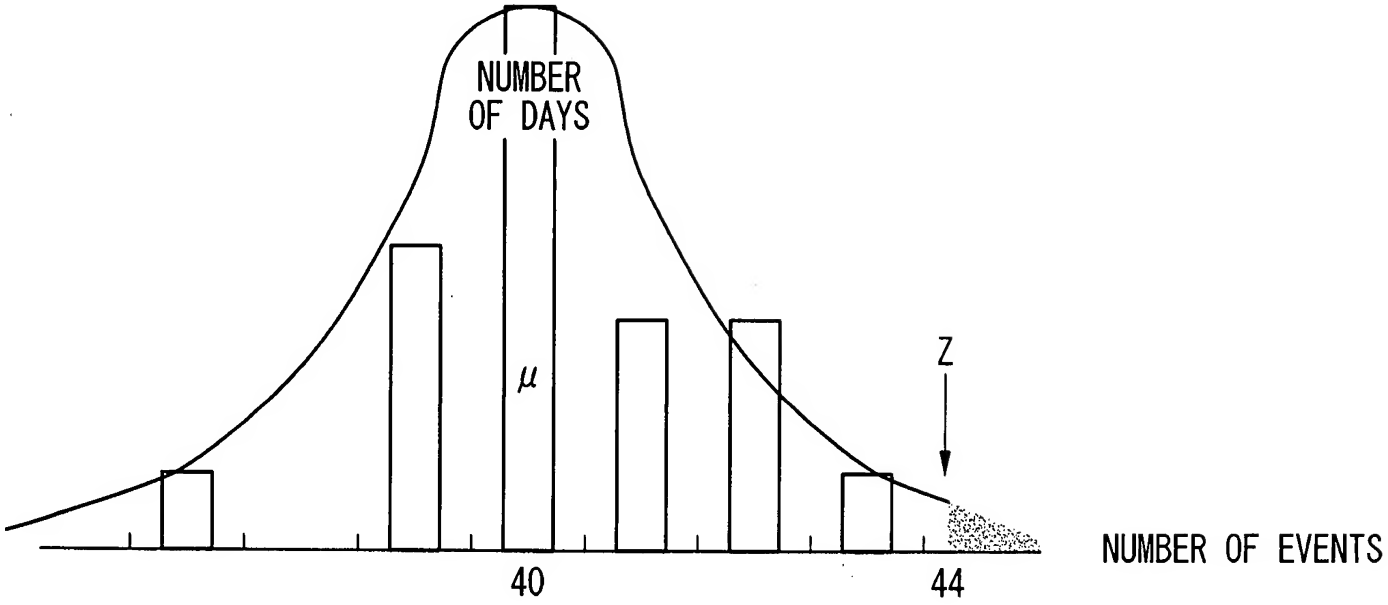
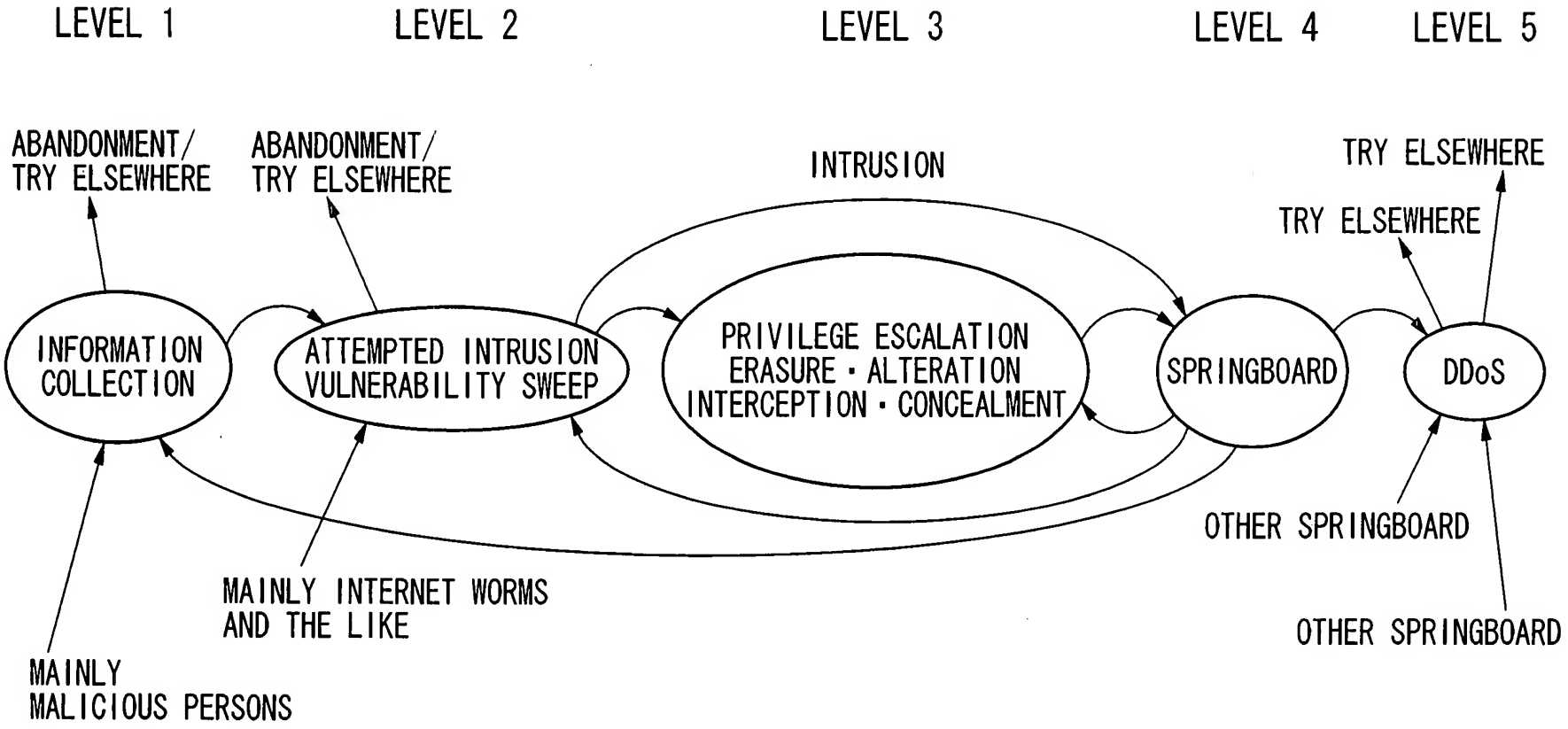


FIG. 8


LEVEL 1
LEVEL 2
LEVEL 3
LEVEL 4
LEVEL 5
ABANDONMENT/
TRY ELSEWHERE
ABANDONMENT/
TRY ELSEWHERE
INTRUSION
TRY ELSEWHERE
TRY ELSEWHERE
INFORMATION
COLLECTION
ATTEMPTED INTRUSION
VULNERABILITY SWEEP
PRIVILEGE ESCALATION
ERASURE · ALTERATION
INTERCEPTION · CONCEALMENT
SPRINGBOARD
DDoS
OTHER SPRINGBOARD
MAINLY INTERNET WORMS
AND THE LIKE
OTHER SPRINGBOARD
MAINLY
MALICIOUS PERSONS